FORTINET

WHITE PAPER

Scaling for High-Performance Security

6 Criteria for Choosing Next-Generation Firewalls

Executive Summary

The shift to a hybrid workforce and the rapid adoption of cloud services have allowed today's users to connect to any resource from any location using any device. While this flexibility is necessary, it also expands the attack surface, opening the door to new threats. Organizations need to be sure their network security enables complete visibility across the entire distributed infrastructure. Otherwise, it will be impossible to effectively deliver and coordinate security protection with fast enough threat detection and remediation.

Next-generation firewalls (NGFWs) provide comprehensive threat protection by adding advanced functionality such as intrusion prevention, application control, content security, web filtering, edge security, and SD-WAN. Advanced NGFWs also inspect secure sockets layer (SSL)/transport layer security (TLS)-encrypted traffic. In some NGFWs, though, the combination of these processes can severely hamper network throughput. That's why, as application counts and traffic volumes grow, security teams may resort to turning off some threat protection controls to maintain acceptable levels of network service.

$4.35 M

According to a recent report, the average cost of a data breach was $4.35 million in 2022[1]

This is a compromise that organizations cannot afford. Next-generation firewalls must offer best-of-breed threat protection at every enterprise edge and in the data center without sacrificing performance. They must also be part of a broad, integrated, and automated security architecture to be effective across the organization. Plus, they should address the scalability, cost of ownership, and environmental concerns of the digitally transforming enterprise.

Requirements for Evaluating NGFWs

Next-generation firewalls play an important role in threat protection, from the network edge to the data center, between internal segments, and in the cloud. Security teams rely on NGFWs to gain visibility into users, devices, applications, and threats on the network, and to apply advanced threat protection wherever it is needed.

Six key criteria should guide the evaluation and selection of NGFWs for enterprise edges or data centers.

1. **Threat protection performance.** Threat protection performance is a measurement of how well an NGFW performs while running full threat protection, including firewalling, intrusion prevention, antivirus, and application control. It is critical for the NGFW to sustain high performance when full threat protection is turned on.

   Many NGFW providers are ambiguous about how they represent their threat protection performance claims. Documented performance claims should be examined carefully to ensure they reflect testing under load, with threat protection fully engaged.

2. **Single-pane-of-glass management.** The management interface is where many security architects are stymied in their selection process. Careful attention may have been paid to the management system's user interface and functionality, but if it is limited to the NGFW, security teams will have to toggle between multiple dashboards to assess vulnerabilities and respond to threats. End-to-end visibility and control are possible only if the NGFW is part of a broad, integrated security architecture, across which it can share threat information with other network devices and receive threat intelligence automatically.

   Single-pane-of-glass management is more effective from a security standpoint and is operationally more efficient, reducing administrative time and training costs.

3. **SSL/TLS 1.3 inspection across the entire enterprise.** An enterprise NGFW must also be able to perform well with SSL inspection engaged. Cybercriminals are taking advantage of the inherent trust and low inspection priority given to SSL traffic by some and are inserting malware into encrypted packets. Such malware can be ferreted out through decryption and inspection.

   An NGFW should have predictable performance and see minimal speed degradation, even with all security services turned on. When comparing vendors, look for transparency in SSL/TLS performance specifications. They should cite testing with industry-mandated ciphers (standardized algorithms used for encrypting and decrypting sensitive information) such as AES256-SHA256, that have preferably been validated by objective third parties.

4. **Secure SD-WAN.** Organizations today depend on redundant WAN internet connections and have distributed offices requiring affordable and resilient SD-WAN solutions. While SD-WAN improves flexibility, scalability, performance, and agility for virtual, edge, branch, and cloud environments, it also opens the door for a new set of security challenges. Although some SD-WAN offerings come with out-of-the-box security features, this add-on security isn't enough to protecting enterprise workloads over a widely distributed network.

   Many NFGW vendors have added SD-WAN features to allow organizations with branch offices to build highly available and high-performance networks. However, these offerings are not ideal. Look for a vendor that offers fully integrated secure SD-WAN capabilities in NGFWs that help consolidate their point products and enforce centralized control. This reduces overall investment costs, while eliminating security gaps.

Almost all internet traffic is now encrypted[2]

5. **Price/performance and other operational considerations.** Some vendors scale performance by increasing the size, and consequently, the price of their NGFWs. This may not align with enterprise trends toward shrinking technology footprints. Aim for an NGFW that delivers the required performance in the most compact form factor. This not only reduces total cost of ownership (TCO) but it also saves space and reduces energy consumption—both important objectives for environmentally conscious enterprises.

   Maintenance and support costs for the NGFW should be factored into TCO, too. Mature technology has an edge in this respect, as does an offering from a vendor with deep investments in research and design. Owners of NGFWs that fall into this category can expect smoother deployments and fewer support calls.

   When considering the NGFW hardware, pay attention to power redundancy and support for 40 GbE and 100 GbE network interfaces. These will support resiliency and accommodate migration to higher-capacity networks.

6. **Independent third-party validation.** Although network security is a rapidly evolving industry, no enterprise can afford the risk of untested security innovations. Architects should not rely on vendor claims alone but seek third-party evaluation from recognized testing houses such as CyberRatings.org.

Top NGFW Priorities

Because the NGFW plays a critical role in protecting the entire enterprise, including corporate and customer data, security architects should be diligent in reviewing their options. When evaluating NGFW solutions, potential trade-offs between security and performance may be top of mind. The ability to provide consistent and consolidated security protection across all distributed edges with minimal performance impact is critical.

There are other considerations, too, however. Given power and space restrictions, preference should be given for compact NGFW solutions that minimize space requirements while being flexible enough to deploy in the data center or on the network edge. And finally, security architects should make sure the NGFW is integrated into the overall security architecture, providing end-to-end visibility and the ability to automatically share threat intelligence between devices.

[1] "Cost of Data Breach Report 2022," IBM, 2022.

[2] "HTTPS encryption on the web," Google Transparency Report, Google, accessed June 2, 2022.

Copyright © 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

June 22, 2023 4:40 PM

2155416-0-0-EN